PROCEDE DE CONTROLE AUTOMATIQUE DES FRAUDES DANS UN SYSTEME DE TRANSACTIONS ELECTRONIQUES

L'invention concerne le domaine des services en ligne sur Internet ou tout autre réseau d'information.

Ces services mettent généralement en jeu des protocoles destinés à préserver la confidentialité des transactions électroniques réalisées. Notamment, ces services garantissent l'anonymat des utilisateurs par l'utilisation de clés de session. Lorsqu'un utilisateur se connecte à un service, une clé de session lui est attribuée. Cette clé est utilisée pour crypter les informations échangées entre l'utilisateur et le système fournisseur de services.

Certains systèmes de services en ligne disposent de moyens pour révéler la clé de session en cas d'utilisation frauduleuse du service. La révélation de la clé de session conduit à la révélation de l'identité de l'utilisateur malhonnête et par conséquent à la levée de l'anonymat de cet utilisateur.

Les moyens de levée d'anonymat d'utilisateurs mettent nécessairement en œuvre des moyens de détection aptes à commander la levée de l'anonymat si certaines conditions d'utilisation frauduleuse sont remplies. Ces moyens doivent donc être aptes à déterminer si il y a utilisation frauduleuse ou non.

Un but de l'invention est de fournir un système de levée d'anonymat dans le cadre d'un service en ligne qui ne nécessite pas de moyens pour déterminer une utilisation frauduleuse.

L'invention s'applique en cas d'utilisation frauduleuse consistant à obtenir un service un nombre de fois supérieur à ce qui est autorisé au cours d'une même session. C'est le cas par exemple, lorsqu'un utilisateur qui se connecte à un site de téléchargement de fichiers obtient le téléchargement de plusieurs fichiers alors qu'en réalité, il n'a payé que pour le téléchargement d'un seul fichier.

L'invention s'applique en particulier à la duplication illicite de biens électroniques.

L'invention propose un procédé de contrôle automatique des fraudes dans un système de transactions électroniques, caractérisé en ce qu'il comprend les étapes consistant à :

- lorsqu'un utilisateur initie une session dans le système de transaction électronique, générer un élément et enregistrer dans une base de données l'élément en association avec des informations identifiant l'utilisateur,

- à chaque fois qu'au cours de la session l'utilisateur commande la réalisation d'une opération, déterminer une équation à laquelle satisfait l'élément enregistré dans la base de données,

- lorsqu'un nombre suffisant donné d'opérations a été effectué, résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément,

- en se reportant à la base de données, déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur.

Dans le cadre de l'invention, une session est définie comme une période de temps au cours de laquelle un utilisateur est en relation avec un service en ligne donné et est autorisé par le fournisseur du service à réaliser un certain nombre d'opérations données.

Le procédé de l'invention conduit à révéler l'identité d'un utilisateur lorsque celui-ci a réalisé un nombre n donné d'opérations au cours d'une même session alors qu'il n'y était pas autorisé par le fournisseur de services.

Le procédé de l'invention s'applique automatiquement et de la même manière à tous les utilisateurs d'un service donné. Il n'y a donc aucune distinction d'application entre utilisateurs frauduleux et utilisateurs normaux. Le procédé de l'invention ne met donc pas en œuvre de moyens spécifiques en cas d'utilisation frauduleuse.

Par ailleurs, avec le procédé de l'invention, l'identité de l'utilisateur n'est divulguée que lorsque celui-ci réalise un nombre donné n d'opérations supérieur au nombre d'opérations autorisé, au cours d'une même session. Par conséquent, avant que l'utilisateur ne réalise la n-ième opération, le procédé ne donne aucune indication quant à l'identité de l'utilisateur

puisqu'il fournit un certain nombre d'équations et qu'il existe une infinité de solutions satisfaisant ces équations. Il en résulte que le procédé de l'invention permet de préserver totalement l'anonymat des utilisateurs tant que ceux-ci respectent les limites définies par le fournisseur de services.

De préférence, les équations du système d'équations sont indépendantes. Ainsi, l'utilisateur sera systématiquement identifié lorsqu'il aura réalisé un nombre n connu d'opérations, le nombre n correspondant au nombre d'opérations nécessaires pour obtenir un système de n équations conduisant à une solution unique.

Les équations peuvent être des équations linéaires.

L'élément est par exemple constitué d'une série de coefficients numériques.

Ces coefficients numériques peuvent avantageusement définir un objet géométrique tel qu'un point, une droite, un hyperplan, etc. dans un espace à n dimensions.

Ils peuvent également définir un objet mathématique tel qu'une fonction, une suite, etc.

L'invention concerne également un système de contrôle automatique des fraudes dans un système de transactions électroniques, caractérisé en ce qu'il comprend des premiers moyens de calcul pour générer un élément lorsqu'un utilisateur initie une session dans le système de transactions électroniques, une base de données dans laquelle est enregistré l'élément en association avec des informations identifiant l'utilisateur, les premiers moyens de calcul étant aptes à déterminer une équation à laquelle satisfait l'élément enregistré dans la base de données à chaque fois qu'au cours de la session l'utilisateur commande la réalisation d'une opération, et des seconds moyens de calcul aptes à résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément lorsqu'un nombre suffisant donné d'opérations a été effectué, de sorte qu'en se reportant à la base de données, il soit possible de déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur.

D'autres caractéristiques et avantages ressortiront encore de la description qui suit, laquelle est purement illustrative et non limitative et doit être lue en regard des figures annexées parmi lesquelles :

- la figure 1 représente un exemple de système conforme à une mise en œuvre de l'invention,
- la figure 2 est une représentation graphique de la détermination d'un élément associé à un utilisateur, l'élément étant une droite définie dans un espace à 2 dimensions,
- la figure 3 est une représentation graphique de la détermination d'un élément associé à un utilisateur, l'élément étant un plan défini dans un espace de dimension n=3,
- la figure 4 est une représentation graphique de la détermination d'un élément associé à un utilisateur, l'élément étant un point défini dans un espace à 2 dimensions,
- la figure 5 est une représentation graphique de la détermination d'un élément associé à un utilisateur, l'élément étant un point défini dans un espace de dimension n=3.

Sur la figure 1, le système de contrôle des fraudes 100 est associé à un serveur 200 de services en ligne (par exemple service de téléchargement de fichiers ou de programmes, service d'achats en ligne, service de consultation de documents, service de communication, etc.) détenu par un fournisseur de services. Le système de contrôle des fraudes comprend un module de pilotage 102 relié au serveur 200, une base de données 104 reliée au module de pilotage 102, un générateur pseudo-aléatoire 106, un premier module de calcul 108 et un deuxième module de calcul 110. Le générateur pseudo-aléatoire 106, le premier module de calcul 108 et un deuxième module de calcul 110 sont commandés par le module de pilotage 102.

Selon une première mise en œuvre du système de l'invention, lorsqu'un utilisateur 300 se connecte au serveur 200 du fournisseur de services via un réseau de communication 400 et ouvre une session, une clé de session temporaire est automatiquement attribuée à l'utilisateur par le serveur. La clé de session est enregistrée dans la base de données 104.

Elle est normalement conservée dans la base de données 104 durant toute la durée de la session, puis supprimée lors de la fermeture de la session. Elle permet un échange sécurisé entre l'utilisateur 300 et le serveur 200. Les clés et autres informations contenues dans la base de données 104 sont confidentielles.

Par ailleurs, lorsque l'utilisateur 300 ouvre une session, le premier module de calcul 108 génère une équation de droite (dimension 1) dans un espace de dimension 2, l'équation étant du type $Y = aX + b$. L'équation de droite est enregistrée dans la base de données 104 en association avec la clé de session attribuées à l'utilisateur. Ainsi, l'utilisateur et la session sont associés de manière univoque à la droite D définie par le couple de coefficients (a, b).

Lorsque l'utilisateur commande la réalisation d'une opération particulière (par exemple téléchargement d'un fichier ou d'un programme) dans le cadre de la session qu'il a ouverte, le premier module de calcul 108 détermine les coordonnées d'un point P_1 (X_1, Y_1) appartenant à la droite D. A cet effet, le module de pilotage commande le générateur pseudo-aléatoire 106 pour que celui-ci génère une première coordonnée X_1. A partir de cette coordonnée X_1, le premier module de calcul 108 détermine une deuxième coordonnée Y_1 à partir de l'équation de la droite D, telle que :

$$Y_1 = aX_1 + b$$

Ce premier point P_1 (X_1, Y_1) seul ne permet pas de déterminer l'équation de la droite D. A ce stade, il n'est pas possible de remonter à l'identité de l'utilisateur 300.

Si l'utilisateur 300 réussit de manière illicite à commander la réalisation d'une autre opération au cours de la même session, le premier module de calcul 108 détermine les coordonnées d'un deuxième point P_2 (X_2, Y_2) appartenant à la droite D. A cet effet, le module de pilotage 102 commande le générateur pseudo-aléatoire 106 pour que celui-ci génère une première coordonnée X_2 différente de X_1. A partir de cette coordonnée X_2, le premier module de calcul 108 détermine une deuxième coordonnée Y_2 à partir de l'équation de la droite D, telle que :

$$Y_2 = aX_2 + b$$

Ainsi qu'illustré sur la figure 2, à partir des deux points P_1 (X_1, Y_1) et P_2 (X_2, Y_2) ainsi déterminés, le deuxième module de calcul 110 en déduit l'équation de la droite D. A cet effet, le deuxième module résout le système d'équations suivant :

$$\begin{cases} Y_1 = aX_1 + b \\ Y_2 = aX_2 + b \end{cases}$$

Connaissant l'équation de la droite D (c'est à dire les coefficients a et b) fournie par le deuxième module de calcul 110, le module de pilotage 102 en déduit, en se reportant à la base de données 104, la clé de session associée. Cette clé permet d'identifier l'utilisateur frauduleux qui a obtenu la réalisation de deux opérations alors même qu'il était autorisé qu'à n'en réaliser qu'une.

Lorsque la confidentialité de l'identité de l'utilisateur 300 a été levée, plusieurs étapes peuvent ensuite être mises en œuvre. Le fournisseur de services peut par exemple interdire à l'utilisateur 300 l'accès au serveur 200.

Dans la mise en œuvre de l'invention décrite précédemment, l'espace dans lequel sont créées des droites est un espace de dimension 2. Cette mise en œuvre peut être généralisée à une application dans un espace de dimension n.

Le premier module de calcul 108 génère une équation d'un hyperplan H (dimension n-1) dans un espace E de dimension n, l'équation étant du type $X_n=a_{n-1}X_{n-1}+...+a_2X_2+a_1X_1+a_0$, dans laquelle au moins (n-2) coefficients parmi a_{n-1}, ..., a_2, a_1, a_0 sont nuls. La clé de session ainsi que l'équation d'hyperplan H associé sont enregistrés dans la base de données 104. Ainsi, l'utilisateur et la session sont associés à l'hyperplan H défini par le n-uplet de coefficients (a_{n-1}, ..., a_2, a_1, a_0).

A chaque fois que l'utilisateur commande la réalisation d'une i-ème opération au cours de la même session, le premier module de calcul 108 détermine un point P_i de coordonnées $(X_i^1, X_i^2, ...X_i^n)$ appartenant à

l'hyperplan H. A cet effet, le module de pilotage 102 commande le générateur pseudo-aléatoire 106 pour que celui-ci génère un (n-1)-uplet de coordonnées $(X_i^1, X_i^2, ...X_i^{n-1})$. A partir de ce (n-1)-uplet, le premier module de calcul 108 détermine une n-ième coordonnée X_i^n en se référant à l'équation de l'hyperplan H, telle que :

$$X_i^n = a_{n-1}X_i^{n-1} + ...a_2X_i^2 + a_1X_i^1 + a_0$$

Lorsque l'utilisateur 300 a commandé pour la n-ième fois la réalisation d'une opération au cours de la même session, le deuxième module de calcul 110 déduit l'équation de l'hyperplan H à partir des n points P_1, P_2,...P_n calculés par le premier module de calcul 108. A cet effet, il résout le système d'équations suivant :

$$\begin{cases} X_1^n = a_{n-1}X_1^{n-1} + ...a_2X_1^2 + a_1X_1^1 + a_0 \\ X_2^n = a_{n-1}X_2^{n-1} + ...a_2X_2^2 + a_1X_2^1 + a_0 \\ ... \\ X_n^n = a_{n-1}X_n^{n-1} + ...a_2X_n^2 + a_1X_n^1 + a_0 \end{cases}$$

Connaissant l'équation de l'hyperplan H (c'est à dire les coefficients a_{n-1}, ..., a_2, a_1, a_0), il est possible, en se reportant à la base de données 104 d'en déduire la clé de session associée à cet hyperplan H et par conséquent de remonter à l'identité de l'utilisateur frauduleux. Cette clé permet d'identifier l'utilisateur frauduleux qui a obtenu la réalisation de n opérations alors même qu'il était autorisé qu'à n'en réaliser que n-1.

La figure 3 représente la détermination d'un plan H (dimension 2) dans un espace de dimension n=3 à partir de 3 points P_1, P_2 et P_3 calculés par le premier module de calcul 108.

Selon un deuxième mode de mise en œuvre du système de contrôle des fraudes, lorsqu'un utilisateur 300 se connecte au serveur 200 du fournisseur de services via un réseau de communication 400 et ouvre une session, une clé de session temporaire est automatiquement attribuée à l'utilisateur 300 par le serveur 200.

Le premier module de calcul 108 génère un point P (dimension 0) dans un espace de dimension 2. Le point étant défini par des coordonnées du type (X, Y). La clé de session ainsi que les coordonnées du point P associées sont enregistrées dans la base de données.

Lorsque l'utilisateur commande la réalisation de l'opération, le premier module de calcul détermine un équation $Y=a_1X+b_1$ d'une droite D_1 passant par le point P (X, Y). A cet effet, le module de pilotage commande le générateur pseudo-aléatoire pour que celui-ci génère un premier coefficient a_1 correspondant à la pente de la droite D_1. A partir de ce coefficient a_1, le premier module de calcul détermine un deuxième coefficient b_1 correspondant à l'ordonnée à l'origine de la droite D_1 à partir des coordonnées (X, Y) tel que $Y=a_1X+b_1$. On a :

$$b_1 = Y - a_1 \cdot X$$

Cette première équation de droite $Y=a_1X+b_1$ ne permet pas de déterminer les coordonnées du point P (X, Y) et de remonter à l'identité de l'utilisateur.

Ainsi qu'illustré sur la figure 4, si l'utilisateur commande de manière illicite la réalisation de la même opération, le premier module détermine une équation $Y=a_2X+b_2$ d'une deuxième droite D_2 passant pas le point (X, Y). A cet effet, le module de pilotage commande le générateur pseudo-aléatoire pour que celui-ci génère un premier coefficient a_2 différent de a_1. A partir de ce coefficient a_2, le premier module de calcul détermine un deuxième coefficient b_2 à partir des coordonnées du point (X, Y) tel que :

$$b_2 = Y - a_2 \cdot X$$

Dans cette mise en œuvre de l'invention, l'espace dans lequel sont créés les points est un espace de dimension 2. Cette mise en œuvre peut être généralisée à une application dans un espace de dimension n.

Lorsque l'utilisateur commande la réalisation d'une opération particulière (par exemple téléchargement d'un fichier ou d'un programme) dans le cadre de la session qu'il a ouverte, le premier module de calcul 108 génère un point P (dimension 0) dans un espace de dimension n. La clé de session ainsi que le point P associé à cette clé sont enregistrés dans la

base de données 104. Ainsi, l'utilisateur et la session sont associés à un point P défini par le n-uplet de coordonnées (X_1, X_2, ...X_n).

A chaque fois que l'utilisateur commande la réalisation d'une i-ème opération au cours de la même session, le premier module de calcul 108 détermine un hyperplan H_i contenant le point P (X_1, X_2, ...X_n), l'hyperplan H_i étant défini par une équation du type $X^n = a_{n-1}^i X^{n-1} + ...a_2^i X^2 + a_1^i X^1 + a_0^i$, dans laquelle au moins (n-2) coefficients parmi les coefficients $a_{n-1}^i, ...a_2^i, a_1^i, a_0^i$ sont nuls. A cet effet, le module de pilotage commande le générateur pseudo-aléatoire 106 pour que celui-ci génère un (n-1)-uplet de coefficients $(a_1^i, a_2^i, ..., a_{n-1}^i)$. A partir de ce (n-1)-uplet, le premier module de calcul 108 détermine un n-ième coefficient a_0^i à partir des coordonnées du point P (X_0, X_1, X_2, ...X_n), tel que :

$$X_n = a_{n-1}^i X_{n-1} + ...a_2^i X_2 + a_1^i X_1 + a_0^i$$

L'anonymat de l'utilisateur 300 est maintenu tant que celui-ci réalise au plus (n-1) opérations car le système génère (n-1) équations à n inconnues, les n inconnues étant les coordonnées (X_1, X_2, ...X_n) du point P.

Lorsque l'utilisateur 300 réalise n opérations au cours de la même session, le deuxième module de calcul 110 déduit les coordonnées du point P (X_1, X_2, ...X_n) comme étant l'intersection des n hyperplans H_1, H_2...H_n calculés par le premier module de calcul 108. A cet effet, le deuxième module de calcul 110 résout un système de n équations à n inconnues :

$$\begin{cases} X_n = a_{n-1}^1 X_{n-1} + ...a_2^1 X_2 + a_1^1 X_1 + a_0^1 \\ X_n = a_{n-1}^2 X_{n-1} + ...a_2^2 X_2 + a_1^2 X_1 + a_0^2 \\ ... \\ X_n = a_{n-1}^n X_{n-1} + ...a_2^n X_2 + a_1^n X_1 + a_0^n \end{cases}$$

Connaissant les coordonnées du point P (X_1, X_2, ...X_n), il est possible, en se reportant à la base de données 104 d'en déduire la clé de

session associée à ce point P et par conséquent de remonter à l'identité de l'utilisateur frauduleux.

La figure 5 représente la détermination du point P dans un espace de dimension n=3 à partir de 3 plans H_1, H_2 et H_3 (dimension 2) calculés par le premier module de calcul 108.

REVENDICATIONS

1. Procédé de contrôle automatique des fraudes dans un système de transactions électroniques, caractérisé en ce qu'il comprend les étapes consistant à :

- lorsqu'un utilisateur initie une session dans le système de transaction électronique, générer un élément et enregistrer dans une base de données l'élément en association avec des informations identifiant l'utilisateur,

- à chaque fois qu'au cours de la session l'utilisateur commande la réalisation d'une opération, déterminer une équation à laquelle satisfait l'élément enregistré dans la base de données,

- lorsqu'un nombre suffisant donné d'opérations a été effectué, résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément,

- en se reportant à la base de données, déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur.

2. Procédé selon la revendication 1, caractérisé en ce que les équations du système d'équations sont indépendantes.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que les équations sont des équations linéaires.

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que l'élément est constitué d'une série de coefficients numériques.

5. Procédé selon la revendication 4, caractérisé en ce que la série de coefficients définit une équation d'hyperplan (H) de dimension (n-1) dans un espace (E) de dimension n et en ce que, à chaque fois que l'utilisateur commande la réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer les coordonnées $(X_i^1, X_i^2, \ldots X_i^n)$ d'un point (P_i) appartenant à l'hyperplan (H).

6. Procédé selon la revendication 5, caractérisé en ce que la série de coefficients définit une équation de droite (D) dans un espace (E) à 2 dimensions et en ce que, à chaque fois que l'utilisateur commande la

réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer les coordonnées (X_i, Y_i) appartenant à cette droite (D).

7. Procédé selon la revendication 4, caractérisé en ce que la série de coefficients définit les coordonnées (X_1, X_2, ...X_n) d'un point (P) dans un espace (E) de dimension n, et en ce que, à chaque fois que l'utilisateur commande la réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer l'équation d'un hyperplan (H_i) contenant le point P.

8. Procédé selon la revendication 7, caractérisé en ce que la série de coefficients définit les coordonnées (X_1, X_2) d'un point (P) dans un espace (E) à 2 dimensions et en ce que, à chaque fois que l'utilisateur commande la réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer l'équation d'une droite (D_i) passant par le point P.

9. Système de contrôle automatique des fraudes dans un système de transactions électroniques, caractérisé en ce qu'il comprend des premiers moyens de calcul (108) pour générer un élément lorsqu'un utilisateur (300) initie une session dans le système de transaction électronique (200), une base de données (104) dans laquelle est enregistré l'élément en association avec des informations identifiant l'utilisateur, les premiers moyens de calcul (108) étant aptes à déterminer une équation à laquelle satisfait l'élément enregistré dans la base de données (104) à chaque fois qu'au cours de la session l'utilisateur (300) commande la réalisation d'une opération, et des seconds moyens de calcul (110) aptes à résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément lorsqu'un nombre suffisant donné (n) d'opérations a été effectué, de sorte qu'en se reportant à la base de données (104), il soit possible de déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur (300).

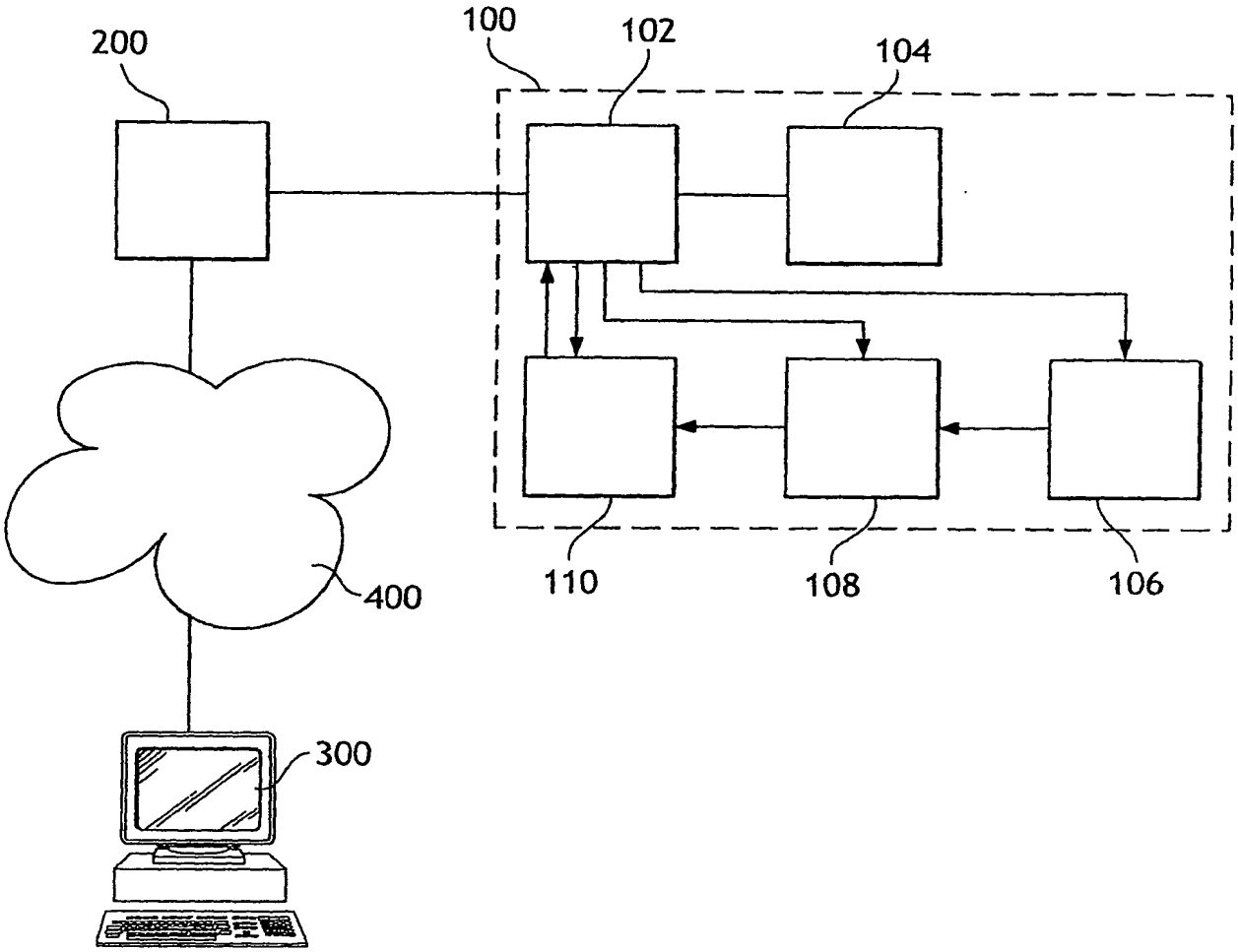

FIG.1

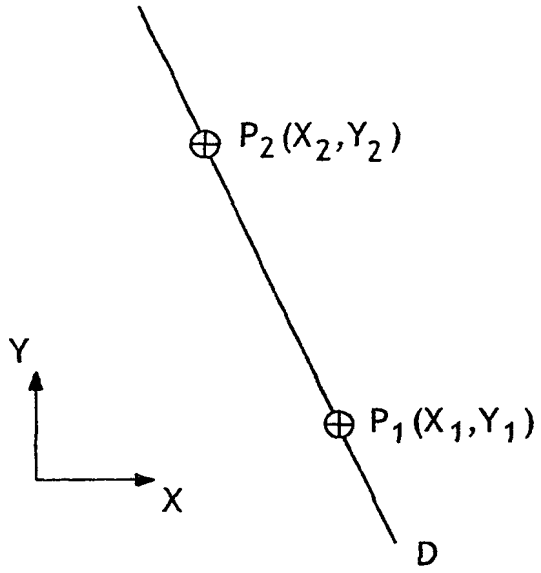
P2 (X2, Y2)
P1 (X1, Y1)
Y
X
D

FIG.2

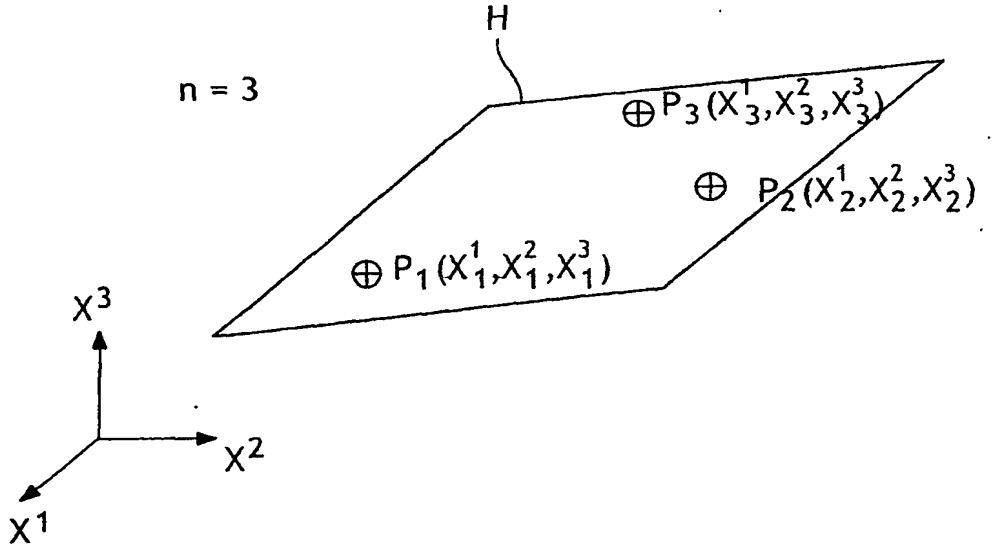
H
n = 3
P3 (X13, X23, X33)
P2 (X12, X22, X32)
P1 (X11, X21, X31)
X3
X2
X1

FIG.3

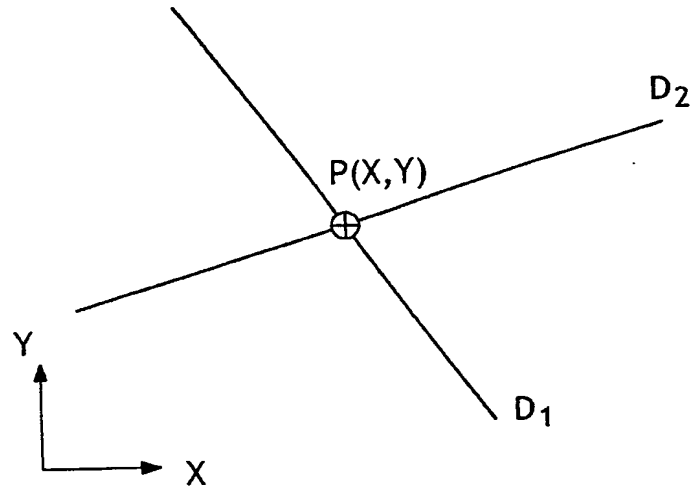

FIG.4

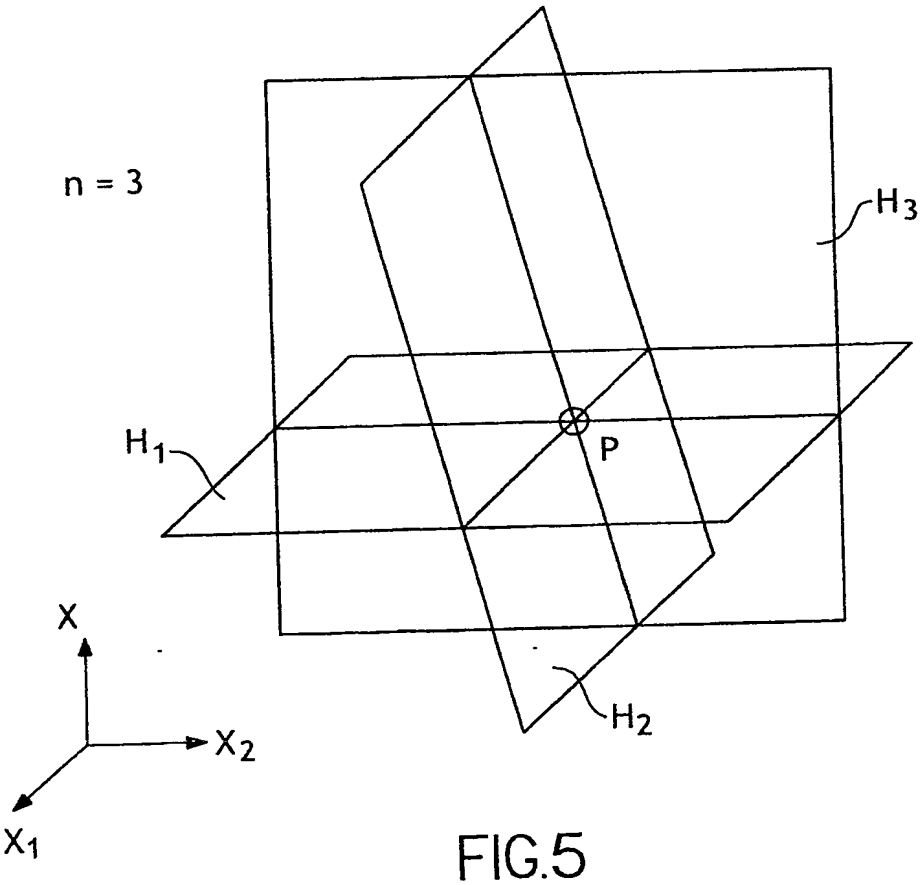

FIG.5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/002734

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L29/06 H04L12/14 G06F17/60 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 636 613 B1 (SCHWENK JOERG ET AL) 21 October 2003 (2003-10-21) abstract column 1, line 65 - column 2, line 30 column 2, line 52 - column 4, line 5	1-9
A	DE 197 50 779 C (DEUTSCHE TELEKOM AG ; DAIMLER BENZ INTERSERVICES DEB (DE)) 14 January 1999 (1999-01-14) column 1, line 5 - line 10 column 1, line 35 - line 40 column 2, line 6 - line 21 column 3, line 25 - column 4, line 45	1-9

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 March 2005	31/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bec, T

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/002734

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 845 267 A (RONEN YZHAK) 1 December 1998 (1998-12-01) abstract column 2, line 25 - column 3, line 12 column 5, line 20 - column 8, line 50 figures 1-3	1-9
A	FIAT A ET AL: "DYNAMIC TRAITOR TRACING" JOURNAL OF CRYPTOLOGY, SPRINGER VERLAG, NEW YORK, NY, US, vol. 14, no. 3, June 2001 (2001-06), pages 211-223, XP001077668 ISSN: 0933-2790 page 215 - page 222	1-9
A	BONEH D ET AL: "An efficient public key traitor tracing scheme" ADVANCES IN CRYPTOLOGY. CRYPTO '99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, CA, AUG. 15 - 19, 1999. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE ; VOL. 1666, BERLIN : SPRINGER, DE, 15 August 1999 (1999-08-15), pages 338-353, XP002273114 ISBN: 3-540-66347-9 page 340 - page 346	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR2004/002734

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6636613 B1	21-10-2003	DE 19847942 A1	13-04-2000
		EP 0993176 A2	12-04-2000
DE 19750779 C	14-01-1999	DE 19750779 C1	14-01-1999
		AU 1666799 A	31-05-1999
		WO 9925090 A1	20-05-1999
		EP 1031205 A1	30-08-2000
		JP 2001523018 T	20-11-2001
		US 6760445 B1	06-07-2004
US 5845267 A	01-12-1998	AU 3819197 A	26-03-1998
		WO 9810382 A1	12-03-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/002734

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/08 H04L29/06 H04L12/14 G06F17/60 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 6 636 613 B1 (SCHWENK JOERG ET AL) 21 octobre 2003 (2003-10-21) abrégé colonne 1, ligne 65 - colonne 2, ligne 30 colonne 2, ligne 52 - colonne 4, ligne 5	1-9
A	DE 197 50 779 C (DEUTSCHE TELEKOM AG ; DAIMLER BENZ INTERSERVICES DEB (DE)) 14 janvier 1999 (1999-01-14) colonne 1, ligne 5 - ligne 10 colonne 1, ligne 35 - ligne 40 colonne 2, ligne 6 - ligne 21 colonne 3, ligne 25 - colonne 4, ligne 45	1-9

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
14 mars 2005	31/03/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bec, T

Formulaire PCT/ISA/210 (deuxième feuille) (Janvier 2004)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2004/002734

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 845 267 A (RONEN YZHAK) 1 décembre 1998 (1998-12-01) abrégé colonne 2, ligne 25 - colonne 3, ligne 12 colonne 5, ligne 20 - colonne 8, ligne 50 figures 1-3	1-9
A	FIAT A ET AL: "DYNAMIC TRAITOR TRACING" JOURNAL OF CRYPTOLOGY, SPRINGER VERLAG, NEW YORK, NY, US, vol. 14, no. 3, juin 2001 (2001-06), pages 211-223, XP001077668 ISSN: 0933-2790 page 215 - page 222	1-9
A	BONEH D ET AL: "An efficient public key traitor tracing scheme" ADVANCES IN CRYPTOLOGY. CRYPTO '99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, CA, AUG. 15 - 19, 1999. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE ; VOL. 1666, BERLIN : SPRINGER, DE, 15 août 1999 (1999-08-15), pages 338-353, XP002273114 ISBN: 3-540-66347-9 page 340 - page 346	1-9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR2004/002734

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 6636613	B1	21-10-2003	DE	19847942 A1	13-04-2000
			EP	0993176 A2	12-04-2000
DE 19750779	C	14-01-1999	DE	19750779 C1	14-01-1999
			AU	1666799 A	31-05-1999
			WO	9925090 A1	20-05-1999
			EP	1031205 A1	30-08-2000
			JP	2001523018 T	20-11-2001
			US	6760445 B1	06-07-2004
US 5845267	A	01-12-1998	AU	3819197 A	26-03-1998
			WO	9810382 A1	12-03-1998